WILLKIE FARR & GALLAGHER LLP
BENEDICT HUR (SBN 224018)
bhur@willkie.com
SIMONA AGNOLUCCI (SBN 246943)
sagnolucci@willkie.com
EDUARDO SANTACANA (SBN 281668)
esantacana@willkie.com
JOSHUA D. ANDERSON (SBN 312836)
jdanderson@willkie.com
TIFFANY LIN (SBN 321472)
tlin@willkie.com
DAVID D. DOAK (SBN 301319)
ddoak@willkie.com
NADIM HOUSSAIN (SBN 335556)
nhoussain@willkie.com
HARRIS MATEEN (SBN 335593)
hmateen@willkie.com
NAIARA TOKER (SBN 346145)
ntoker@willkie.com
333 Bush Street, 34th Floor
San Francisco, CA 94104
Telephone: (415) 858-7400
Facsimile: (415) 858-7599

Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JOHN DOE I, et al., individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No. 3:23-cv-02431-VC
(Consol. w/ 3:23-cv-02343-VC)

DEFENDANT GOOGLE LLC'S SUPPLEMENTAL BRIEF RE: MARCH 20, 2025 ORDER REQUESTING FURTHER BRIEFING

Ctrm: 4 – 17th Floor (San Francisco)
Before: District Judge Vince Chhabria

Consol. Complaint Filed: July 13, 2023
2nd Am. Complaint Filed: August 12, 2024

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. Introduction

In its March 20, 2025 Order Requesting Further Briefing, Dkt. No. 191, the Court requested supplemental briefing on Google's Motion to Dismiss the Second Amended Complaint (SAC), Dkt. No. 164. The Court enumerated the following issues related to the fundamental question of whether the SAC "adequately alleged that Google has obtained [Plaintiffs'] private health information in a way that enables Google to actually identify them and link the information to them":

1. whether it can be inferred from the allegations in the SAC that (a) the gid cookie or (b) the cid cookie sends Google private health information that Google can tie to a user's identity;

2. whether a reasonable person could conclude that Google's Privacy Policy (a) "promised to only collect health information after consent by users" and that (b) "the health information at issue here was covered by that promise"; and

3. whether the SAC adequately alleges intent (a) before the 2023 HIPAA disclosure, and (b) after the 2023 HIPAA disclosure.

On the Court's first question, the allegations of the SAC themselves do not go so far as to assert facially that the gid cookie sends information "in a way that enables Google to actually identify [users] and link the information to them." Instead, as it does regarding other cookies, the SAC alleges that the gid cookie *could* under certain circumstances be used to tie information to a particular user's identity subject to various controls, including the optional, default-*off* "Google Signals" setting that all Google Analytics developers have available to them. SAC ¶ 97. Leaving aside the inaccuracy of these allegations, the SAC does not allege that any of the subject healthcare websites ever turned Google Signals *on*. Nor does the SAC come anywhere near alleging facts from which an inference could be drawn that any of the subject healthcare websites turned Google Signals on, such as, for example, that information from those websites was saved in a user's Google Account, or that someone experienced advertising suggesting that such information was used to target advertising. Absent such allegations, the most that can be inferred from the SAC is that the system worked as designed (and as Google publicly commits to it working), which is that

it does not track or exploit private health information.

The Court's second question focuses on a phrase that Plaintiffs misleadingly excerpted from Google's Privacy Policy. Plaintiffs' interpretation misses the mark. In the Privacy Policy, the specific promise in question is in fact limited in scope to information collected "in the course of using Google services that offer health-related features, such as the Google Health Studies app." No reasonable person could read this promise to apply to Google Analytics. Further, the SAC fails adequately to allege a breach.

The Court's third question reiterates that something other than providing a product that functions responsibly out of the box is required to infer that Google intended to receive identifiable private health information. The Court identifies the 2023 HIPAA disclosure as sufficient evidence that Google, post-2023, did not plausibly intend to receive identifiable private health information (absent competent fraud allegations). So too before 2023, when Google's HIPAA disclosure made the same points, albeit in a different place on its website. And Google also made those points in its terms of use, the contract it entered into with each website developer.

Further, the SAC fails adequately to allege that the product, as it is designed, will automatically send identifiable private health information to Google; without irresponsible customization in contravention of Google's terms of use, no such transgression can occur.

Finally, the Court appears in its Order to apply a foreseeability standard for intent, but the Court's analysis of the willfulness requirement for CIPA makes clear that bare foreseeability alone should not be enough to impose a duty to warn, lest Google then be liable for the independent actions of third parties. Even if it is foreseeable that a product can be misused, that does not mean that failure to warn not to use it that way amounts to criminal intent.

For these reasons, Plaintiffs fall short of alleging plausibly that Google acted with the intent to receive identifiable private health information. The inferences required to believe otherwise are unreasonable and unwarranted in this case.

II. It cannot be inferred from the SAC that Google received private health information.

As an initial matter, the SAC fails plausibly to allege that private health information was sent to Google in the first place. As the Court notes, the SAC's best allegation that "health information" was transmitted to Google is a single excerpt from an inadmissible[1] expert report that misleadingly suggests a cookie ID attempted to book a urology appointment. The URL, which anyone can follow,[2] leads to a public directory entry for a specific physician, and clicking the "Schedule Appointment" button leads to a phone number pop-up a user should call to schedule. This does not constitute "health information" in any sense. It is general web browsing activity, it is not an authenticated webpage, and it does not reveal any fact relating to the user's medical history or status. Nor does clicking on this button make the user "identifiable" in any respect, or even narrow the field of people whom the user might be. Indeed, all humans could use a urologist, and even if the physician's specialty implied a focus on a subset of humanity (like a gerontologist could imply a focus on older adults), that hardly narrows down anything about that user that constitutes health information; at most, a URL like this *could* convey general demographic information like age or sex, none of which constitutes health information, and it could just as easily imply only that someone was surfing the web who does not even fall into the relevant category.

Indeed, HHS addressed this exact question, and concluded in its informal guidance that something more than visiting an appointment page is required, such as the collection of the user's subjective reason for visiting that page, e.g., "tracking technologies might collect an individual's email address, or *reason for seeking health care typed or selected by an individual*, when the individual visits a regulated entity's webpage and makes an appointment with a health care provider or enters symptoms in an online tool to obtain a health analysis." Dkt. No. 165-11 at 5 (emphasis added). In *American Hospital Association v. Becerra*, the Northern District of Texas

[1] *See* Mot. to Dismiss SAC at 9 n.2 Dkt. No. 164 (citing cases holding that expert reports generated for litigation are not appropriate attachments to a complaint and should not be considered).

[2] *See* https://providers.gundersenhealth.org/provider/joseph-m-endrizzi/2091914.

agreed that even information showing that an individual visited a page for booking a specific type of appointment would not constitute individually identifiable health information ("IIHI").[3] 738 F. Supp. 3d 780, 802 (N.D. Tex. 2024) (quoting from the hospitals' brief, which stated information showing "that John Smith visited a page for booking dialysis appointments . . . that establishes nothing."). There is no allegation in the SAC, nor excerpt in the inadmissible expert report attached to it, suggesting that symptoms, unredacted patient records, or billing information were ever transmitted alongside a URL indicating that a user was on an appointment page or any other similar page.

For this reason, the Court's analysis could stop here. Absent a competent allegation that actual health information snuck into the pipeline of data, contrary to Google's policies and the obligations of the healthcare providers themselves, the questions regarding whether such information was identifiable and whether Google intended for it to sneak through are irrelevant.

III. It cannot be inferred from the SAC that Google received identifiable information.

The allegations of the SAC do not support the inference that the gid cookie (or the cid cookie) is used by Google to personally identify private health information. To the contrary, the SAC itself acknowledges that there are certain optional, non-default conditions that must be met for such linking to occur, and it fails to allege facts from which it could be inferred that any of those non-default conditions were present here.

In its Order, the Court reasons that the gid cookie "seems to collect information that, when a website interaction involves Google account holders, can link that website interaction to those account holders in a way that identifies them." Dkt. No. 191 at 2. For support, the Court notes that Plaintiffs allege that the cookie generates a unique identifier that "can be tied to that user's Google account." *Id.* But the SAC's allegations are more nuanced than that, in dispositive ways.

[3] Plaintiffs have not alleged that Google is subject to HIPAA, and their definition of "health information" in the SAC is far more expansive than that of HIPAA's. SAC ¶ 21; Dkt. No. 184 at 43 (Ms. Gardner: "Our [sic] definition of health information incorporates HIPAA and the FTCs . . . . [i]t is pretty broad, you know, reasonable but broad definition of health.").

The heart of Plaintiffs' identifiability argument is at paragraph 109 of the SAC, where they summarize that there are two arguments they pose for identifiability. First, they argue that "identifiers on their own can identify a unique individual." This corresponds to their allegation at paragraphs 101 through 104, for example, that an IP address and various other identifiers, including both the cid and gid cookies, *by themselves* constitute identifiable information. The Court's Order appears to reject that argument, reasoning that the cid cookie, for example, is admittedly a "synonymized cookie, i.e., one that is assigned to a particular user but does not collect any information that could be used to identify a person in the real world." Dkt. No. 191 at 3. This conclusion is correct: without a plausible allegation that synonymized information, or as the E.U. and California call it, "pseudonymized" information,[4] was re-associated with a user's true identity, there is no basis to infer that the presence of such identifiers alone constitutes identifiable information.[5]

Plaintiffs' second argument summarized in paragraph 109 of the SAC is that even if the identifiers like the gid cookie value are not by themselves personally identifiable, they are rendered so because "Google can combine those identifiers with other information in its possession, to

[4] *See, e.g.*, Cal. Civ. Code § 1798.140(aa) (CCPA) ("'Pseudonymize' or 'Pseudonymization' means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer."); Regulation (EU) 2016/679 (General Data Protection Regulation) ("GDPR") Art. 4(5) ("'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person").

[5] The Google Help Page that Plaintiffs cite in support of their description of cid describes the cid cookie as "pseudonymous," though Plaintiffs conveniently omit that word when quoting from that page. *Compare* SAC ¶ 97 ("the cid field 'identifies a particular user, device, or browser instance'") Dkt. No. 159-3, *with* Dkt. 158-8 ("[the cid field] *pseudonymously* identifies a particular user, device, or browser instance." (emphasis added)). Further, Plaintiffs' examples of cid and gid cookie values show that they are no more than random strings of numbers. *See, e.g.*, SAC ¶ 89 Dkt. No. 159-3.

further associate the data intercepted from health Care Providers with profiles it maintains about that specific individual." With respect to the gid cookie, the most salient factual allegation supporting this claim is the allegation at paragraph 97, from which the Court's tentative conclusion appears to stem, that the gid cookie is a unique identifier that can be used in conjunction with Google Signals to target advertising.[6] Plaintiffs further explain at paragraph 105, where they distinguish Google account holders from non-holders, that "Google's ability to identify the individuals to whom the transmissions pertain is also evident in the 'Google Signals' program, which provides Health Care Providers with the option to 'better understand your customers across devices using Google's signed-in data.'"

The allegation that Google has special ability to link health information to a Google account holder thus hinges on paragraph 105's explanation of how Google Signals works. But Google Signals is optional; that same paragraph explains that Google Signals must be "activated" by the developer. Absent such activation, which the SAC does not allege to have occurred, the SAC does not identify any aspect of Google's system that, as designed, links analytics data to the individual who generated it. Paragraphs 106-108 accuse Google of maintaining tables that a nefarious actor could use to circumvent Google's policies, but there is no allegation that such a circumvention has ever happened, or if it did, to whom and what, if any, harm came of it.

The conclusion that Plaintiffs draw that cookies like the gid cookie can be used by Google to link user data to the user's identity by virtue of their having a Google account is thus hypothetical. It depends either on the developer activating Google Signals *or* on a nefarious actor circumventing Google's data security and policies. Plaintiffs do not allege that either circumstance

[6] The only support Plaintiffs cite for their explanation of the gid cookie in paragraph 97 is not a Google Help page, but rather an third-party webpage discussing an inapplicable ruling by the Austrian Data Protection Authority under the GDPR. SAC ¶ 97 n.28. Plaintiffs did not seek judicial notice of this webpage nor attach it to the SAC, and in any event, the webpage stops short of concluding that the gid cookie constitutes personally identifiable information. *See id.* ("It is therefore possible that these identifiers would be considered personal data. . . . this does not mean that they *for sure would be*.") (emphasis in original).

occurred as to any named Plaintiff, any member of the proposed class, or any of the thousands of websites they identify in their SAC.

Granted, a plaintiff cannot be expected to know the precise account control settings of healthcare websites, but where the setting is not on by default, and must be activated by that developer, *some* fact should be alleged to indicate that such a thing occurred, such as that a user received an untoward advertisement, or that the information showed up in their Google Account history (where other Google Signals information would be expected to show up).

And, in fact, there are further hypotheticals upon which such an inference depends. Paragraph 105 and the page Plaintiffs cite for their discussion of Google Signals explain that the user must also have opted into certain features for such linking to occur at all, including the "Ads Personalization" feature.[7] That page in turn links to further help-center pages explaining that some ad topics are off limits, and others are customizable (such as opting into receiving ads about weight loss). Plaintiffs do not allege whether they have opted into the "Ads Personalization" feature, nor that they received any unwanted advertisements.

This recalls another central problem with Plaintiffs' pleading. The SAC selectively relies on sections of Google's help center, taking what it says as true, while ignoring other sections of it that explain that Google does not use health information to target advertising. Like reading only certain pages of a user manual, the picture the SAC creates is confusing and misleading. And even still, it falls short of giving rise to an inference that any identifiable information was actually sent to Google by any website developer.

Ultimately, as with the question of whether health information was sent, the issue here is that Plaintiffs' theory of liability depends not on anything Google did, but on the independent actions of third parties (and of themselves) that have not been pleaded. Out of the box, Google Analytics doesn't collect identifiable health information, no matter the webpage it's installed on.

[7] *See* SAC ¶ 105 n.30 (citing https://support.google.com/analytics/answer/7532985); Dkt. No. 165-9 at 2.

And the SAC doesn't allege that third parties (the web developers and the users) took any of the steps that would have been necessary to circumvent that out-of-the-box behavior.

IV. The SAC fails plausibly to allege that Google breached a promise.

The Court's Order notes that "it appears that the plaintiffs may have stated a claim" for breach of contract based on the Privacy Policy section called "Information We Collect," which lists among other categories of information:

> **Health information** if you choose to provide it, such as your medical history, vital signs and health metrics (like blood glucose levels), and other similar information related to your physical or mental health, in the course of using Google services that offer health-related features, such as the Google Health Studies app.

See ECF 191 at 3 (citing Dkt. No. 158-14 at 19).

Plaintiffs omit whenever possible the final clause of the sentence, but the final clause plainly cabins the scope of the alleged promise to data collected in the course of using "Google services that offer health-related features, such as the Google Health Studies app." Nothing in the SAC gives rise to an inference that Plaintiffs' use of a *third party's* website constitutes their "using *Google* services that offer health-related features, such as the Google Health Studies app." Dkt. No. 158-14 at 19 (emphasis added). Nor could it; this provision is plainly meant to disclose that Google may collect "medical history, vital signs and health metrics" when users use Google services designed to collect such information. No reasonable person could conclude that this provision was meant also to promise something about what Google would or would not receive via Google Analytics.

Indeed, Google addresses Google Analytics elsewhere in its Privacy Policy, in sections that make no promise about health information. There was no reason to make such a promise because Google does not intend to receive health information via Google Analytics *at all*, not just when users do not consent to it. The reason Plaintiffs cannot maintain a breach of contract claim based on the Privacy Policy is because there is no promise that addresses the subject matter of this case. What the Privacy Policy does promise is that Google will not use health information to target advertising, Dkt. No. 158-14 at 30 ("We don't use topics or show personalized ads based on

sensitive categories like race, religion, sexual orientation, or health. And we require the same from advertisers that use our services."). There are no facts in the SAC that would support an allegation that Google breached that promise.

And, even if a reasonable person could read the passage above to apply to data sent via Google Analytics, as discussed above, the SAC fails to allege that identifiable health information was actually received by Google, so there could be no breach. *Supra* Section III. Certainly, nothing in the SAC or its attachments comes close to the "medical history, vital signs, and health metrics (like blood glucose levels), and other similar information" that is the subject of the purported promise. At most, as discussed above, Plaintiffs allege that a single "schedule appointment" on an unauthenticated directory of physicians that leads to a phone number was transmitted to Google, and Plaintiffs do not allege facts from which it could be inferred that Google Signals, which is off by default, was enabled by that healthcare provider, nor that any of the named Plaintiffs visited that specific webpage after opting in to the "Ads Personalization" setting in their Google account. The fact that a user clicks on a link leading to a phone number for a physician, even if that user action *were* identifiable with a specific user, is nowhere near the itemized list of types of health information covered by the purported promise.

V. Google never intended to collect identifiable health information.

On the subject of intent, which underlies all the remaining claims, the Court concludes that Plaintiffs failed to allege that Google acted "consciously and deliberately with the goal of intercepting wire communications" for the time period post-dating the 2023 HIPAA disclosure. Dkt. No. 191 at 4. The Court reasons that the intent required here is the intent to collect "communications about private health information that Google can link to a particular, identifiable individual." *Id.* The Court notes that it does not matter for this lawsuit "whether Google intended to intercept other types of communications" and that "even if Google intended to intercept communications about private health information (which it denies), that wouldn't matter for purposes of this suit if Google couldn't link the information to a particular, identifiable person." *Id.*

This is the correct standard. Out of the box, Google Analytics is agnostic as to the subject matter of the website on which it's installed. It works the same by default whether installed by a sneaker company or a hospital, and the SAC does not deny that, by default, Google Analytics is not designed to capture user input on something like a hospital's web portal *at all*. Instead, the most that can be said is that the SAC alleges that Google Analytics by design captures URLs from page visits, which should never contain private health information; after all, a URL is simply the address of the visited page, not the content of the communications exchanged with the website owner on that page.

Applying this intent standard (and note, for CIPA, that the higher "willfulness" standard applies), the Court concludes that the 2023 HIPAA disclosure negates intent because it demonstrates that Google "told providers not to use Google's products on any page that may be related to the provision of health care services," thus obviating the possibility that health information would make its way into the data stream. *Id.* at 5. But, the Court concludes, Google's failure to "explain to providers how to avoid sharing private health information about identifiable Google account holders through the gid cookie" *before* 2023 renders it reasonable to infer that Google intended to collect identifiable health information, since "[i]t was obvious that some of these communications [sent by Google Analytics] would be between patients and providers" so it was "therefore obvious that some of them would disclose private health information. *Id.* at 5.

In this, the Court is making inferences the SAC does not support. Even setting aside any HIPAA disclosure, the obligation to abide by HIPAA is not Google's; it belongs to healthcare providers. Google provided a free tool to all web developers that was agnostic as to subject matter. That it may have been "obvious" that hospital websites would use it does not mean that it was also obvious that they would customize it in ways that would risk violating their own privacy obligations, and contrary to Google's terms of use, such that the tool would capture "communications . . . between patients and providers," nor was it obvious that "some of them would disclose private health information" because, as discussed above, nothing about Google Analytics is designed, by default, to capture user input, messages exchanged on a website, test

results, or anything else that could be considered to constitute health information. Indeed, this is evident from the conspicuous lack of allegations, or evidence in the attachments to the SAC, of actual health information being transmitted to Google. If communications between patients and their doctors were being captured, or if true health information were disclosed, Plaintiffs would have pleaded it—they have, after all, had several chances to do so.

Moreover, even if Google knew healthcare providers were capable of *misusing* Google Analytics to capture such communications, that alone does not rise to the level of willful intent required by, for example, CIPA, nor the lower intent standards of other claims. The Court's reasoning borders on imposing on Google a duty to warn its customers of the myriad ways in which they could misuse the product, an affirmative duty that Plaintiffs have already conceded does not exist.[8] There is no case cited in the briefing that would support such a low standard for intent, especially in the context of a criminal statute. If that were the standard, then tape-recorder manufacturers could have the requisite mens rea to be guilty of unlawful recordings made by their customers. However obvious it was that healthcare providers would use Google Analytics, that does not mean it was also obvious that they would misuse it.

Regardless, if the 2023 HIPAA disclosure is enough to negate Google's intent after 2023, the 2018 HIPAA disclosure and the Terms of Use for Google Analytics were sufficient to negate Google's intent before 2023.

The 2018 HIPAA disclosure contains all the same critical warnings of the 2023 disclosure. That policy guide addressed to Google Analytics customers was titled "Best practices to avoid sending Personally Identifiable Information (PII)." In it, Google stresses in a bolded "HIPAA Disclaimer" section:

> Unless otherwise specified in writing by Google, Google does not intend uses of Google Analytics to create obligations under the Health Insurance Portability and Accountability Act, as amended, ("HIPAA"), and makes no representations that Google Analytics satisfies HIPAA requirements. If you

[8] Dkt. No. 184 at 6 (The Court: "I assume there is no affirmative duty to warn healthcare providers. You agree with that? Ms. Gardner: Correct, Your Honor.").

> are (or become) a Covered Entity or Business Associate under HIPAA, you may not use Google Analytics for any purpose or in any manner involving Protected Health Information unless you have received prior written consent to such use from Google.

Dkt. No. 165-5 at 4. The same document also warns that "you may not send Google Analytics encrypted Protected Health Information (as defined under HIPAA), even if it is hashed or salted." *Id.*

If Google's duty was to warn that Google Analytics could be misused, e.g., "in any manner involving Protected Health Information," then it discharged that duty in this 2018 document. To the extent Plaintiffs' argument is that the warning was inadequately worded, that does not translate into an affirmative intent to collect "communications about private health information that Google can link to a particular, identifiable individual." Order, Dkt. No. 191 at 4. At most, it amounts to an argument that Google could have added more detail to the 2018 disclosure, which is nowhere near the intent required, and certainly is not a crime.

The pre-2018 disclaimer is also plenty similar to the 2023 disclosure the Court relies on. In the 2023 disclosure, Google again warns that "HIPAA-regulated entities using Google Analytics must refrain from exposing to Google any data that may be considered Protected Health Information (PHI)" and points to and summarizes the HHS bulletin that did not exist before the update to the HIPAA disclosure. Dkt. No. 165-3. Both documents also warn customers not to send *any* information that could be construed as personally identifiable information ("PII"). And both documents advise customers to consult with their legal teams if they have questions about how to comply with their privacy obligations.

Google also, at all relevant times, contractually *required* its customers to not send it PII, to disclose their use of Google Analytics, and to obtain consent where legally necessary, including to the use of Google Analytics cookies. The contract obligates customers as follows:

- "You will not and will not assist or permit any third party to, pass information to Google that Google could use or recognize as personally identifiable information."
- You "will comply with all applicable laws, policies, and regulations relating to the collection of information from Users."

- "You must post a Privacy Policy and that Privacy Policy must provide notice of Your use of cookies, identifiers for mobile devices . . . or similar technology used to collect data."

- "You will use commercially reasonable efforts to ensure that a User is provided with clear and comprehensive information about, and consents to, the storing and accessing of cookies or other information . . . and where providing such information and obtaining such consent is required by law."

- "You must not circumvent any privacy features (e.g., an opt-out) that are part of the Service."

Dkt No. 165-2 at 4 (2019 Google Analytics Terms of Service). In other words, Google evinced a clear and unbroken line of intent *not* to receive health information and *not* to receive PII. There is no fact alleged in the SAC that undermines this clear, unbroken pattern of honorable intent.

Finally, the Court notes in its analysis that the upshot of the 2023 disclosure was that, by advising that Google Analytics not be included on "any page that may be related to the provision of health care services," Google was "prevent[ing] the gid cookie from sending personal health information in a way that would allow Google to link it to identifiable Google account holders because the cookie would not be on any page containing personal health information." Dkt. No. 191 at 5. That is one way to prevent the gid cookie from collecting identifiable health information. But there were also other ways that Google could, and did, prevent this from happening, as described above:

- By its design, Google Analytics does not send Google health information, and Plaintiffs do not allege otherwise, other than that it sends URLs from visited pages, which Plaintiffs fail to allege resulted in the sending of actual health information in any real instance;

- By its design, Google Analytics does not tie information to a user's identity; instead, only when various optional, off-by-default conditions are met can such a tying occur, including that the developer affirmatively chooses to do so;

- Google does not target advertising based on sensitive health information;

- The Google Analytics Terms of Service and policies prohibited developers from sending Google personally identifiable information;

- The Google Analytics Terms of Service required developers to disclose their use of Google Analytics and obtain consent where legally necessary, including to the use of cookies.

These facts bolster the conclusion that the SAC as alleged negates the element of willfulness or intent here, particularly where Google instructed healthcare providers to refrain from sending Google personally identifiable information, to disclose their use of Google Analytics, and to obtain user consent where legally necessary. *See, e.g.*, *B.K. v. Desert Care Network*, No. 2:23-cv-05021, 2024 WL 5338587, at *3 (C.D. Cal. Aug. 22, 2024) (dismissing CIPA 631 claim alleging Meta received sensitive health information from healthcare provider websites via the Meta Pixel because "the SAC does not allege that Meta knew or should have known that the data it received from Defendants was collected without users' consent.").

As it stands, the SAC alleges nothing more than that Google's agnostic analytics product could, hypothetically, be misused, without alleging that it was misused, by whom, or how, without alleging that Google knew about the misuse, and without alleging that Google failed to make appropriate policies to forbid the sending of identifiable information and health information. These facts do not add up to "conscious and deliberate" conduct with the goal to collect "communications about private health information that Google can link to a particular, identifiable individual."

VI. Conclusion

The SAC fails even to allege that, out of thousands of websites, Plaintiffs were able to uncover any actual health information that was transmitted to Google: no symptoms, no health metrics, no vital signs, no health conditions, no messages with physicians, nothing. Nor have they alleged any facts suggesting that even if such health information was transmitted, that Google identified it as belonging to a particular individual. As for the contract claim, the purported promise Plaintiffs rely upon is incomplete, and when considered in its entire context, does not apply to this case. Indeed, Google had no reason to promise it would not collect health information via Google Analytics because it had no reason to believe there was a risk it might happen, given its policies, the default design of analytics, and the obligations that apply to those who manage health information. And, of course, even if the promise had been made, Plaintiffs fail to allege a breach.

Nor does the SAC allege facts from which intent can be inferred. Plaintiffs' intent argument amounts to an argument that the misuse of Google Analytics was foreseeable. Even if it was, that does not rise to the level of the intent standard that applies to Plaintiffs' claims. And regardless, such misuse was not foreseeable, because Google took steps before and after 2023 to inform customers that they should not send health information to Google via Google Analytics, and given the legal obligations that apply to managers of health information, it was not incumbent on Google under any law to assume such entities would fail to meet those obligations and misuse the product nevertheless.

For these reasons, the Court should dismiss the Second Amended Complaint with prejudice.

Dated: March 27, 2025

WILLKIE FARR & GALLAGHER LLP
Benedict Hur
Simona Agnolucci
Eduardo Santacana
Joshua Anderson
Tiffany Lin
David Doak
Nadim Houssain
Harris Mateen
Naiara Toker

By: */s/ Eduardo Santacana*
Eduardo Santacana

Attorneys for Defendant
GOOGLE LLC